Vol. 6 - N.º 1 (enero/junio 2026) ISSN 2718-8582 URI: https://id.caicyt.gov.ar/ark:/s27188582/tsfamo7rv

Vacíos de marco regulatorio ante amenazas híbridas: ciberterrorismo bajo la figura del narcotráfico en México

Carlos Ramírez Castañeda[1]

Universidad Abierta y a Distancia de México, México

Recibido: 03 de marzo de 2026
Aceptado: 26 de mayo de 2026

Creative Commons 4.0

Cómo citar: Ramírez Castañeda, C. (2026). Vacíos de marco regulatorio ante amenazas híbridas: ciberterrorismo bajo la figura del narcotráfico en México. *Revista Pares - Ciencias Sociales, 6*(1), 81-89. ARK CAICYT: https://id.caicyt.gov.ar/ark:/s27188582/tsfamo7rv

Resumen

La convergencia entre dinámicas del narcotráfico y fenómenos de agresión digital ha configurado un tipo de riesgo compuesto que presiona las capacidades estatales en México. El objetivo central de este artículo es determinar en qué medida el marco jurídico mexicano presenta vacíos estructurales para atender conductas digitales con finalidad intimidatoria o de desestabilización institucional vinculadas al narcotráfico, y proponer líneas mínimas de adecuación normativa compatibles con el sistema constitucional de garantías. El análisis examina las amenazas híbridas mediante un análisis jurídico-documental de carácter exploratorio-analítico que revisa categorías conceptuales (terrorismo, ciberterrorismo, cibercrimen y delincuencia organizada) y normas aplicables (Código Penal Federal, Ley Federal contra la Delincuencia Organizada, Ley de Seguridad Nacional, Código Nacional de Procedimientos Penales CNPP y Ley Federal de Telecomunicaciones y Radiodifusión). Los hallazgos revelan un tratamiento fragmentario y reactivo, con vacíos definicionales y la ausencia de un marco integral de prevención y respuesta. Se proponen cuatro líneas de adecuación normativa: la tipificación autónoma del ciberterrorismo (art. 139 Ter CPF), la reforma al artículo 139 para incluir medios digitales, la creación de una Agencia Nacional de Ciberseguridad y la incorporación de obligaciones de reporte para operadores de sectores críticos con salvaguardas de derechos humanos.

Palabras clave: amenazas híbridas, ciberterrorismo, narcotráfico, delincuencia organizada, infraestructura crítica, ciberseguridad, México

Legal and regulatory gaps in Mexico facing hybrid threats: cyberterrorism and drug trafficking

Abstract

This convergence between drug trafficking dynamics and digital aggression phenomena has configured a composite type of risk that pressures state capacities in Mexico. The central objective of this article is to determine the extent to which the Mexican legal framework presents structural gaps in addressing digital conduct with an intimidatory or institutionally destabilizing purpose linked to drug trafficking, and to propose minimum normative adaptations compatible with constitutional system of guarantees. Through a documentary legal analysis of an exploratory-analytical character, the study reviews conceptual categories (terrorism, cyberterrorism, cybercrime, organized crime) and applicable provisions (Federal Criminal Code, Federal Law against Organized Crime, National Security Law, National Code of Criminal Procedure, Federal Telecommunications and Broadcasting Law). The findings reveal a fragmented and reactive approach, with definitional gaps and the absence of an comprenhensive framework for prevention and response. Four minimum normative lines are proposed: the autonomous criminalization of cyberterrorism (FCC art. 139 Ter), the reform of Article 139 to include digital means, the creation of a National Cybersecurity Agency, and the establishment of mandatory reporting obligations for critical-sector operators with explicit human rights safeguards.

Keywords: hybrid threats, cyberterrorism, drug trafficking, organized crime, critical infrastructure, cybersecurity, Mexico

[1] Es investigador en la Universidad Abierta y a Distancia de México (UnADM). Es Licenciado en Derecho por la Universidad Nacional Autónoma de México; Máster en Derecho de las Nuevas Tecnologías de la Información y Comunicaciones por el IECS, Santiago de Compostela, España; Doctor en Administración y Políticas Públicas, y cuenta con un Posdoctorado en Derecho por el Centro de Estudios Superiores Jurídicos y Criminológicos.

Su trabajo académico se centra en el análisis jurídico de las tecnologías emergentes, la ciberseguridad, el ciberterrorismo y los impactos del delito organizado en entornos digitales, con especial énfasis en derechos humanos, debido proceso y regulación tecnológica. Ha desarrollado y difundido contenidos académicos y de divulgación sobre riesgos, desafíos y tendencias del cibercrimen aplicados al contexto mexicano. Sus líneas actuales de investigación abordan las amenazas híbridas, el cibercrimen, la protección de derechos fundamentales en entornos digitales y los vacíos regulatorios en México frente al avance tecnológico.

ORCID: https://orcid.org/0000-0002-3400-3408

Correo electrónico: cybercrimemx@hotmail.com

Lacunas no marco regulatório diante de ameaças híbridas: ciberterrorismo e narcotráfico no México

Resumo

A convergência entre dinâmicas do narcotráfico e agressões digitais configura um tipo de risco composto que pressiona as capacidades estatais no México. O objetivo central deste artigo é determinar em que medida o marco jurídico mexicano apresenta lacunas estruturais para tratar condutas digitais com finalidade intimidatória ou de desestabilização institucional vinculadas ao narcotráfico, e propor linhas mínimas de adequação normativa compatíveis com as garantias constitucionais. O estudo examina as ameaças híbridas por meio de uma análise jurídico-documental de caráter exploratório-analítico que revisa categorias conceituais (terrorismo, ciberterrorismo, cibercrime e criminalidade organizada) e disposições jurídicas aplicáveis (Código Penal Federal, Lei Federal contra a Delinquência Organizada , Lei de Segurança Nacional, Código Nacional de Procedimentos Penais e Lei Federal de Telecomunicações e Radiodifussão). Os achados revelam um tratamento fragmentário e reativo, com lacunas definicionais e ausência de um marco integral de prevenção e resposta. Propõem-se quatro linhas mínimas de adequação normativa: tipificação autônoma do ciberterrorismo (art. 139 Ter), reforma do artigo 139 para incluir meios digitais, criação de uma Agência Nacional de Cibersegurança e obrigações de notificação para operadores de setores críticos com salvaguardas explícitas de direitos humanos.

Palavras-chave: ameaças híbridas; ciberterrorismo; narcotráfico; criminalidade organizada; infraestrutura crítica; cibersegurança; México

Introducción

Durante las últimas décadas, el Estado mexicano ha enfrentado un desafío sostenido: la violencia vinculada al narcotráfico y la diversificación de formas de coacción sobre instituciones y comunidades. Este fenómeno, además de su dimensión territorial, ha incorporado un componente comunicacional y tecnológico que amplifica el miedo social, debilita la confianza pública e interfiere con funciones estatales. Paralelamente, el incremento de ciberincidentes como vulneraciones a bases de datos gubernamentales, suplantación de identidad y campañas dirigidas de intimidación digital, ha sido abordado predominantemente como delincuencia informática, sin considerar de manera suficiente la finalidad intimidatoria o de desestabilización institucional cuando estas conductas se vinculan con estructuras del narcotráfico.

Bajo esta premisa, el artículo analiza la hipótesis de que México enfrenta amenazas híbridas entendidas como formas de agresión que combinan violencia física, control territorial, propaganda intimidatoria y operaciones en el ciberespacio. Estas acciones, al difundirse mediante plataformas digitales, pueden magnificar su impacto social e institucional.

El propósito no consiste en equiparar todo ciberincidente con un delito informático ni en ampliar de manera indiscriminada el derecho penal, sino en identificar cuándo determinadas conductas digitales pueden integrarse en lógicas de desestabilización institucional o terror social. Esta delimitación permite evidenciar carencias regulatorias que requieren atención normativa sin afectar los principios de legalidad, proporcionalidad, debido proceso y protección de derechos humanos.

El vacío jurídico se hace presente cuando la respuesta normativa se fragmenta en categorías que, por separado, no contemplan el impacto ni la finalidad intimidatoria de determinadas conductas ejecutadas mediante medios digitales. En consecuencia, la conceptualización tradicional del terrorismo debe revisarse con cautela para evitar tanto la impunidad por inadecuación típica como la expansión indebida del poder punitivo del Estado.

A partir de lo anterior, la pregunta principal de investigación es la siguiente: ¿en qué medida el marco jurídico mexicano presenta vacíos estructurales para atender conductas digitales con finalidad intimidatoria o de desestabilización institucional vinculadas al narcotráfico? Como pregunta secundaria se plantea: ¿qué líneas mínimas de adecuación normativa pueden formularse sin comprometer derechos humanos, legalidad penal y debido proceso? La contribución del artículo se concentra en identificar zonas grises de regulación vinculadas con definiciones, tipicidad, competencia institucional, infraestructura crítica, capacidades de respuesta, cooperación internacional y control democrático.

Metodología

Se lleva a cabo un análisis jurídico-documental de carácter exploratorio-analítico. El enfoque es exploratorio porque la convergencia entre ciberterrorismo y narcotráfico constituye un área emergente con escaso desarrollo doctrinal en el ordenamiento mexicano (Hernández Sampieri et al., 2014); es analítico-interpretativo en cuanto examina el tenor literal y el alcance teleológico de las disposiciones normativas vigentes para determinar su capacidad de subsunción ante escenarios híbridos. El diseño articula categorías conceptuales con el ordenamiento positivo para mapear estructuralmente sus insuficiencias, método identificado como análisis funcional del derecho (Ferrajoli, 2011).

1. Revisión conceptual de categorías relevantes (terrorismo, ciberterrorismo, cibercrimen, delincuencia organizada, amenazas híbridas).
2. Identificación y lectura de normas mexicanas pertinentes, particularmente el régimen de terrorismo, y figuras relacionadas al Código Penal Federal.

3. Análisis del régimen de delincuencia organizada como marco de persecución de estructuras criminales.

El corpus normativo revisado comprende: Código Penal Federal [CPF] (arts. 139-139 Quáter y 211 bis 1-7); Ley Federal contra la Delincuencia Organizada [LFCDO]; Ley de Seguridad Nacional [LSN] (arts. 5-6); Código Nacional de Procedimientos Penales [CNPP] (arts. 291-295 y cadena de custodia de evidencia digital); y Ley Federal de Telecomunicaciones y Radiodifusión [LFTR] (art. 190). La revisión de cada ordenamiento siguió un esquema analítico uniforme: (i) identificación del bien jurídico tutelado; (ii) elementos del tipo o de la facultad normativa; y (iii) evaluación de su capacidad de subsunción ante escenarios híbridos. La selección de fuentes internacionales como UNTOC/Palermo y Convenio de Budapest, obedece a criterios explícitos: la UNTOC es vinculante para México desde 2003; el Convenio de Budapest constituye un referente internacional para la cooperación penal y la preservación de evidencia digital en materia de ciberdelincuencia (Consejo de Europa, 2001). La Directiva NIS2 (Unión europea, 2022) no se toma como modelo trasplantable por las diferencias de integración supranacional, sino como parámetro comparado sobre gobernanza de riesgos, obligaciones de reporte y protección de sectores esenciales. El marco de Colombia (Ley 1273/2009) se incorpora como referente regional de mayor proximidad sistémica.

Para los efectos de este artículo, el término "vacío regulatorio" se opera bajo tres supuestos que pueden concurrir de manera individual o acumulativa:

1. ausencia de tipo penal que describa de forma completa la conducta analizada;
2. ambigüedad o indeterminación de un elemento normativo que impide la subsunción típica sin incurrir en analogía in malam partem, prohibida por el artículo 14 constitucional; y
3. inexistencia de obligaciones preventivas exigibles jurídicamente para sectores o instituciones determinadas.

Esta definición operacional es coherente con el concepto de laguna jurídica desarrollado por Bobbio (1960) y adaptado al contexto del derecho penal de la tecnología por Miró Llinares (2012).

Ciberterrorismo, narcotráfico y amenazas híbridas: precisiones necesarias

El término ciberterrorismo suele emplearse con diversas acepciones y con una amplitud mediática que exige cautela conceptual para evitar tanto la subestimación del riesgo como la sobrecriminalización. Para efectos de este trabajo, el ciberterrorismo se entiende como el conjunto de actos o amenazas realizados mediante o contra sistemas informáticos con la finalidad de infundir terror, intimidar colectivamente o coaccionar a la autoridad, con impacto real o potencial sobre bienes jurídicos esenciales y sobre el funcionamiento institucional.

Esta definición permite fijar un criterio funcional de análisis, ya que no toda conducta digital ilícita puede considerarse ciberterrorismo. La calificación jurídica depende de la finalidad intimidatoria o de desestabilización, del bien jurídico afectado y del contexto organizacional en que se produce la conducta.

El concepto de ciberterrorismo suele referirse a una serie de acciones muy diferentes, desde la simple difusión de propaganda en línea, hasta la alteración o destrucción de información, e incluso la planificación y ejecución de ataques terroristas mediante el uso de redes informáticas. Así, para comprender mejor qué es el ciberterrorismo, este artículo comenzará analizando el concepto de "terrorismo" (incluyendo su estructura, principio de daño y elementos) como una categoría amplia a la que pertenece la especie "ciberterrorismo"; posteriormente, delimitará la idea de ciberterrorismo y la distinguirá de otras con las que tiene cierta similitud; finalmente, planteará algunos de los desafíos más importantes que implica el ciberterrorismo en un mundo global y tecnológicamente interconectado.

La distinción entre cibercrimen y ciberterrorismo resulta jurídicamente relevante porque determina el bien jurídico tutelado, la finalidad típica y el régimen de investigación aplicable. El cibercrimen suele vincularse con lucro, extorsión, acceso indebido o afectación patrimonial; en cambio, en el ciberterrorismo la dimensión intimidatoria o de desestabilización institucional ocupa el lugar central, aun cuando las acciones se cometan mediante sistemas o medios informáticos.

El cibercrimen engloba cualquier actividad delictiva que utiliza dispositivos electrónicos o redes digitales para realizar fraudes, robos de identidad, extorsiones, o accesos no autorizados a información confidencial. Estos crímenes pueden ir desde el hackeo de cuentas personales hasta ataques masivos contra empresas y gobiernos.

Por ello, la diferencia conceptual no es meramente terminológica: incide en la forma de subsumir la conducta, en la competencia de las autoridades, en los estándares probatorios y en los límites constitucionales de la respuesta penal.

Ahora bien, en paralelo, el narcotráfico en México debe entenderse como una práctica que puede tener ciertos rasgos de gobernanza criminal, al generar mecanismos de control social, intimidación y disciplinamiento comunitario (a veces en mayor escala). Bajo esa lógica, lo comunicacional es totalmente estratégico, pues no solo se busca un beneficio económico del mercado de lo ilícito (drogas, armas, etc.), sino la capacidad de imponer reglas, inhibir autoridades y condicionar decisiones en el plano de lo público.

Aquí es donde las tecnologías digitales por su avance, velocidad y alcance amplifican ese objetivo intimidatorio, ya sea mediante amenazas masivas, difusión de contenidos con el fin de coaccionar o acciones que afectan sistemas de instituciones gubernamentales y/o de sectores críticos.

Finalmente, las amenazas híbridas pueden entenderse como formas de agresión que combinan tácticas físicas, comunicacionales y digitales, con efectos acumulativos sobre capacidades estatales, legitimidad institucional y derechos. Bajo esta premisa, la convergencia entre narcotráfico y operaciones digitales exige un enfoque jurídico que no se limite a perseguir delitos informáticos aislados, sino que considere el contexto de criminalidad organizada, la finalidad intimidatoria, la afectación institucional y

la necesidad de prevención y ciberresiliencia posterior al incidente.

Impactos sobre el Estado mexicano: de la violencia territorial a la presión digital

La influencia del narcotráfico sobre México se traduce en presiones continuas sobre autoridades locales, afectación al control y seguridad del territorio, debilitamiento de servicios públicos, y deterioro de la confianza social. Cuando se marca está dinámica de convergencia y se incorporan medios digitales, el daño se amplifica exponencialmente y el mensaje de intimidación alcanza nuevas audiencias fuera de las fronteras, y se replica rápidamente, produciendo efectos de afectación social. Lo anterior puede derivar en el ejercicio deficiente de funciones públicas, afectación a procesos administrativos e incluso en la inexistencia de la autoridad estatal.

Al hablar del ciberespacio como un ámbito de encuentro y acercamiento con una población, la dependencia creciente en el uso de sistemas digitales incrementa la superficie de vulnerabilidad del Estado y de sectores claramente estratégicos. Sin afirmar que todo ciberincidente constituye terrorismo, puede sostenerse que existe un umbral cualitativo cuya superación transforma la naturaleza de la conducta. Cuando el impacto trasciende el daño al sistema informático específico y afecta la continuidad de funciones estatales esenciales o produce terror colectivo, la conducta adquiere la dimensión del ciberterrorismo (Denning, 2000; Mayer Lux, 2018). Este umbral no es cuantitativo sino teleológico: lo que importa es la finalidad intimidatoria o desestabilizadora. La distinción es jurídicamente relevante porque determina el tipo penal aplicable, la competencia institucional y el régimen de cooperación internacional activable. Ignorarla conduce a dos errores igualmente costosos: impunidad por inadecuación típica o sobrecriminalización por analogía prohibida (Ferrajoli, 2011).

Con ello, surge la imperiosa necesidad de revisar si el marco normativo ofrece herramientas coherentes para clasificar, investigar y responder a estos supuestos, y si existen obligaciones de prevención y reporte hacia sectores críticos.

La vinculación entre violencia física y presión digital constituye un fenómeno verificable en contextos de criminalidad organizada. Por ello, resulta necesario analizar las herramientas jurídicas disponibles para determinar si permiten atender supuestos de ciberterrorismo asociado al narcotráfico sin forzar la interpretación de tipos penales diseñados para otros escenarios.

Marco jurídico mexicano aplicable: legislación existente y límites prácticos

El marco jurídico relacionado con el Derecho penal mexicano incluye diversos tipos vinculados al terrorismo y conductas relacionadas, sin embargo, un problema central en escenarios digitales es la subsunción, pues estos tipos tradicionales se estructuran a partir de acciones que involucran violencia o amenazas en términos tradicionales (en el plano físico únicamente, dejando el plano digital en un segundo término, incluso reduciendo su importancia). La mención del ordenamiento como punto de partida tradicional del terrorismo se aprecia en el siguiente fragmento:

"Artículo 139: Se impondrá pena de prisión de quince a cuarenta años y multa de cuatrocientas a mil doscientas veces el valor diario de la Unidad de Medida y Actualización, sin perjuicio de las penas que correspondan por otros delitos que resulten:

I. A quien utilizando sustancias tóxicas, armas químicas, biológicas o similares, material radioactivo, material nuclear, combustible nuclear, mineral radiactivo, fuente de radiación o instrumentos que emitan radiaciones, explosivos, o armas de fuego, o por incendio, inundación o por cualquier otro medio violento, intencionalmente realice actos en contra de bienes o servicios, ya sea públicos o privados, o bien, en contra de la integridad física, emocional, o la vida de personas, que produzcan alarma, temor o terror en la población o en un grupo o sector de ella, para atentar contra la seguridad nacional o presionar a la autoridad o a un particular, u obligar a éste para que tome una determinación.

II. Al que acuerde o prepare un acto terrorista que se pretenda cometer, se esté cometiendo o se haya cometido en territorio nacional.

Las sanciones a que se refiere el primer párrafo de este artículo se aumentarán en una mitad, cuando, además:

I. El delito sea cometido en contra de un bien inmueble de acceso público;

II. Se genere un daño o perjuicio a la economía nacional, o

III. En la comisión del delito se detenga en calidad de rehén a una persona.

A quien utilice aeronaves pilotadas a distancia para cometer las conductas previstas en la fracción I del párrafo primero del presente artículo, se aumentará hasta en un tercio la pena establecida."

Como se puede apreciar, no existe referencia directa a la disrupción causada por sistemas informáticos: primer gran vacío estructural. La SCJN ha interpretado el artículo 139 CPF señalando que el tipo exige como elemento subjetivo específico la finalidad de atentar contra la seguridad nacional o presionar a la autoridad (Suprema Corte de Justicia de la Nación, 2016). La jurisprudencia no ha resuelto si los medios digitales encuadran en la cláusula "cualquier otro medio violento", generando inseguridad jurídica que inhibe de facto la persecución penal bajo este tipo. Esta laguna no puede resolverse por vía de interpretación analógica sin vulnerar el principio de legalidad estricta (art. 14 constitucional); su solución requiere reforma legislativa explícita (Bobbio, 1960).

Otra de las referencias sobre el delito relacionado con terrorismo dentro del Código Penal Federal se encuentra en el siguiente artículo:

"Artículo 211 bis 1.- Al que sin autorización modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática protegidos por algún mecanismo de seguridad, se le impondrán de seis meses a dos años de prisión y de cien a trescientos días multa. Al que sin autorización conozca o copie información contenida en sistemas o equipos de informática protegidos por algún mecanismo de seguridad, se le impondrán de tres meses a un año de prisión y de cincuenta a ciento cincuenta días multa."

Las disposiciones del artículo 211 bis 1 protegen únicamente la integridad y confidencialidad de los sistemas, sin incorporar la dimensión de la finalidad intimidatoria o coacción institucional. El Primer Tribunal Colegiado en Materia Penal del Primer Circuito ha precisado que la protección del precepto recae en la integridad del sistema informático y no en el contenido comunicacional ni en la finalidad política de la conducta (Primer Tribunal Colegiado en Materia Penal del Primer Circuito, 2012, Tesis I.1o.P.83 P). La pena máxima de dos años contrasta con la de cuarenta del artículo 139: esta brecha de 38 años sin tipo intermedio evidencia la ausencia de una escala punitiva proporcional y constituye, desde la perspectiva del artículo 22 constitucional, una asimetría normativa estructural que requiere reforma mediante la creación de un tipo autónomo de ciberterrorismo.

Con este primer caso del ordenamiento Federal mexicano, es evidente que no se contempla la figura del "miedo digital" y los canales de disrupción que utilizan grupos delincuenciales, en especial los del narcotráfico para sembrar terror.

La LFCDO estructura el tratamiento de organizaciones criminales y habilita un régimen procesal e institucional para su persecución. Resulta relevante cuando la agresión digital forma parte de un patrón de criminalidad organizada, pero no sustituye la necesidad de un ordenamiento integral de ciberseguridad ni resuelve los vacíos de coordinación interinstitucional.

La LSN resulta relevante porque su artículo 5 incluye entre las amenazas a la seguridad nacional "actos que impidan a las autoridades actuar contra la delincuencia organizada" y "actos tendentes a obstaculizar o bloquear actividades de inteligencia o contrainteligencia" (Ley de Seguridad Nacional, 2005). Una campaña de interferencia digital contra sistemas de inteligencia policial podría encuadrar en esta disposición. Sin embargo, la LSN no crea tipos penales autónomos: su función es la atribución de competencias de inteligencia y coordinación interinstitucional. Este límite fue identificado por Cossío Díaz (2011) como uno de los problemas estructurales de la legislación de seguridad mexicana: la multiplicación de marcos que definen amenazas sin crear los tipos penales ni los mecanismos procesales para su persecución.

El CNPP contempla técnicas especiales de investigación en sus arts. 291-295, que incluyen la intervención de comunicaciones privadas y la infiltración de agentes (Código Nacional de Procedimientos Penales, 2014). Su aplicación en contextos de ciberterrorismo presenta tres limitaciones estructurales: exigen autorización judicial previa con causa probable específica, lo que dificulta su uso en tiempo real; presentan problemas de jurisdicción cuando los servidores están en el extranjero; y no existen mecanismos expeditos de requerimiento de datos a plataformas extranjeras sin representación legal en México, brecha identificada por la OCDE (2019) como el principal obstáculo procesal en investigaciones de cibercrimen transnacional.

La LFTR, en su artículo 190, obliga a los concesionarios a colaborar con las autoridades en la localización geográfica en tiempo real de dispositivos (Ley Federal de Telecomunicaciones y Radiodifusión, 2014). Su cobertura se limita a concesionarios sujetos a regulación mexicana, excluyendo sistemáticamente a plataformas como WhatsApp, Telegram y Signal solo por mencionar algunos de los canales preferidos del narcotráfico para sus campañas de intimidación digital. Esta brecha regulatoria es reconocida por la Relatoría Especial para la Libertad de Expresión de la CIDH (2022) como factor que dificulta la investigación de amenazas digitales en América Latina sin comprometer la privacidad de las comunicaciones.

La Estrategia Nacional de Ciberseguridad identifica líneas generales de acción y reconoce la transversalidad del fenómeno digital; sin embargo, su naturaleza es estratégica y programática, no legislativa. Desde la lógica de los vacíos regulatorios, el punto crítico es que una estrategia pública no crea por sí misma obligaciones exigibles, competencias precisas, estándares mínimos de protección, mecanismos de reporte ni responsabilidades jurídicas específicas (Gobierno de México, 2017).

La Estrategia Nacional de Ciberseguridad establece la visión del Estado mexicano en la materia y reconoce tres elementos relevantes:

1. La importancia de las tecnologías de la información y comunicación (TIC) como un factor de desarrollo político, social y económico en México; en el entendido de que cada vez más individuos están conectados a Internet y que tanto organizaciones privadas como públicas desarrollan sus actividades en el ciberespacio.
2. Los riesgos asociados al uso de las tecnologías y el creciente número de ciberdelitos.
3. Las necesidades de una cultura general de ciberseguridad.

El aumento de riesgos, amenazas y ataques informáticos sofisticados, así como el surgimiento de nuevas formas y técnicas para aprovechar vulnerabilidades, así como el incremento de conductas delictivas que se cometen a través de las TIC, son circunstancias que hacen de la ciberseguridad un tema complejo. A lo anterior se suma la naturaleza global del ciberespacio y la concurrencia de diferentes soberanías y marcos jurídicos.

Ninguno de los instrumentos mencionados incorpora una regulación específica del ciberterrorismo ni una definición normativa que permita distinguirlo con claridad de la ciberdelincuencia común. Esta ausencia conduce a un plano interpretativo incierto en la práctica institucional y constituye uno de los vacíos que requiere atención legislativa.

Dentro de las zonas grises podemos identificar la falta de definiciones legales claras para fenómenos o amenazas híbridas, en particular la ausencia evidente de una categorización jurídica de "ciberterrorismo" o de los supuestos de coacción digital con afectaciones sociales, institucionales, y otras variantes lo que produce incertidumbre. En algunos casos se fuerza la subsunción a tipos no diseñados para lo digital, en otros se trata como una categoría relacionada con la cibercriminalidad y los delitos informáticos, lo que resulta en una lectura completamente distinta. Por ello, el riesgo inverso es expandir el concepto de terrorismo de manera vaga, con potenciales afectaciones a la libertad de expresión y al debido proceso.

Con todo y los constantes esfuerzos de Organizaciones Internacionales, Estados y otros sectores interesados, más allá de

la academia no ha sido posible superar las limitaciones dadas por la carencia de un criterio unificado.

La ausencia de criterios homogéneos en políticas públicas y legislación dificulta la identificación de los vacíos regulatorios. Por ello, el análisis posterior se concentra en las insuficiencias normativas que afectan la tipicidad, la coordinación institucional, la infraestructura crítica y la cooperación internacional.

Vacíos a nivel digital e impacto de las carencias jurídicas

La arquitectura normativa mexicana actual tiende a segmentar el problema: terrorismo por una vía, delitos informáticos por otra y delincuencia organizada como marco complementario. Ante amenazas híbridas, esta fragmentación puede impedir apreciar el daño agregado sobre el Estado, pues no solo se afecta un sistema informático, sino también la continuidad institucional, la confianza pública y la producción de miedo colectivo cuando intervienen estructuras vinculadas al narcotráfico.

La tutela incompleta impacta en la priorización institucional, la coordinación interinstitucional y la construcción de casos sólidos para eventuales reformas legislativas. También obliga a considerar la evidencia digital como componente transversal de investigación, aunque su desarrollo técnico-procesal excede el objeto central de esta publicación.

Un vacío estructural es la falta de un régimen plenamente articulado sobre infraestructura crítica, definiciones sectoriales, gestión de riesgos digitales, continuidad operativa y obligaciones de prevención, reporte y respuesta ante ciberincidentes. En un contexto de alta conectividad social, el alcance de las operaciones digitales asociadas a estructuras criminales exige un marco normativo coherente y verificable.

Las amenazas híbridas suelen tener elementos transfronterizos, lo cual exige una cooperación internacional ágil y especializada. No obstante, México carece de un instrumento internacional vinculante específicamente orientado al ciberterrorismo, por lo que la cooperación debe apoyarse en marcos más amplios de ciberdelincuencia, delincuencia organizada y asistencia jurídica internacional.

La respuesta regulatoria no puede basarse en categorías amplias que faciliten arbitrariedades. La experiencia comparada muestra que la mezcla imprecisa de seguridad nacional, terrorismo, desinformación, narcotráfico y orden público puede abrir márgenes de restricción indebida a derechos humanos. Por ello, cualquier adecuación normativa debe sustentarse en legalidad estricta, proporcionalidad, control judicial, transparencia y rendición de cuentas.

En materia de delincuencia organizada transnacional, la Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional (UNTOC) es un eje de cooperación y de entendimiento común del fenómeno. En ciberdelincuencia, el Convenio de Budapest se mantiene como referente de cooperación penal y preservación de evidencia digital, aun cuando los debates nacionales sobre adhesión y armonización requieren un análisis contextual. Estas referencias son útiles no para "trasplantar" modelos, sino para incorporar prácticas de cooperación, estándares de preservación y garantías procesales compatibles con el marco constitucional mexicano.

Para incorporar una propuesta de atención a los vacíos legislativos identificados, resulta pertinente examinar referentes internacionales y comparados que permitan orientar la adecuación normativa sin trasladar mecánicamente modelos ajenos al contexto mexicano.

Marco de referencia internacional para el caso concreto

La Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional (UNTOC), también conocida como Convención de Palermo, resulta relevante para el caso mexicano no porque sea un instrumento cibernético, sino porque ofrece una arquitectura jurídica de cooperación aplicable a fenómenos complejos donde convergen organizaciones criminales, operaciones transfronterizas y la necesidad de asistencia jurídica internacional.

En este sentido, la asistencia jurídica mutua puede facilitar investigaciones, procesos y actuaciones judiciales contra grupos de delincuencia organizada que utilicen medios digitales, especialmente cuando sea necesario preservar, obtener o intercambiar evidencia digital.

Ante amenazas híbridas en las que la atribución puede dispersarse entre operadores del crimen organizado, actores vinculados al narcotráfico y conductas digitales de finalidad intimidatoria, este marco de cooperación puede aportar bases para extradición, asistencia jurídica y coordinación interestatal.

En el plano práctico, la Convención no resuelve por sí misma los desafíos técnicos de ciberseguridad ni crea estándares específicos sobre ciberterrorismo. Su valor es estructural: ofrece bases de cooperación para investigar organizaciones delictivas complejas y evitar que los hechos sean tratados como eventos aislados.

En un país con alta incidencia de criminalidad organizada transnacional, los controles de cooperación internacional deben orientarse a fortalecer la investigación y persecución de estructuras criminales, no a reproducir estereotipos sociales o enfoques meramente declarativos.

Un segundo instrumento relevante es el Convenio sobre la Ciberdelincuencia del Consejo de Europa, conocido como Convenio de Budapest. Para este artículo, su utilidad no radica en regular directamente el ciberterrorismo como tipo autónomo, sino en ofrecer un marco de cooperación penal, preservación de evidencia digital y armonización mínima de capacidades procesales frente a delitos cometidos mediante sistemas informáticos (Consejo de Europa, 2001).

México ha participado históricamente en discusiones sobre el Convenio de Budapest, pero no cuenta con adhesión plena al instrumento. Esta situación limita el acceso directo a ciertos mecanismos de cooperación especializada; no obstante, el Convenio conserva valor como parámetro técnico-jurídico para fortalecer la investigación de ciberdelitos y la obtención transfronteriza de evidencia digital.

Estas referencias no deben entenderse como modelos para copiar de manera automática. Su utilidad consiste en orientar criterios de cooperación, preservación de evidencia, armonización normativa y salvaguardas procesales compatibles con la realidad constitucional mexicana.

Con base en el diagnóstico anterior, se proponen cuatro líneas de adecuación normativa mínima, diferenciadas por objeto y nivel de urgencia. El criterio de 'mínimo' responde a la advertencia de Ferrajoli (2011) sobre los riesgos del punitivismo expansivo: las reformas deben limitarse a lo estrictamente necesario para colmar los vacíos identificados, sin ampliar discrecionalmente el poder punitivo del Estado.

La ausencia de un marco normativo preciso para el ciberterrorismo vinculado al narcotráfico tiene consecuencias directas sobre la eficacia de la respuesta estatal y sobre la protección de derechos fundamentales. Por ello, las líneas propuestas requieren desarrollo normativo, presupuesto específico, formación especializada del personal de procuración de justicia y controles democráticos efectivos. La experiencia comparada muestra que las reformas aisladas, sin acompañamiento institucional y presupuestario, producen tipos penales que no se aplican y organismos que no funcionan (Lessing, 2018; Rid, 2013).

Propuesta mínima de adecuación normativa

1. Tipificación autónoma del ciberterrorismo. Se propone incorporar un artículo 139 Ter al Código Penal Federal para sancionar, con legalidad estricta y finalidad específica, a quien mediante sistemas informáticos, redes de comunicación, datos, plataformas digitales o infraestructura tecnológica realice actos dirigidos a infundir terror en la población, coaccionar a la autoridad o desestabilizar funciones estatales esenciales, siempre que exista afectación real o riesgo jurídicamente relevante sobre servicios públicos, infraestructura crítica, seguridad nacional o derechos fundamentales.

2. Reforma al artículo 139 del CPF. La cláusula de medios violentos debe actualizarse para incluir expresamente medios digitales o tecnológicos cuando se utilicen con finalidad terrorista. Esta reforma evitaría forzar la interpretación de la expresión 'cualquier otro medio violento' y reduciría el riesgo de analogía in malam partem, prohibida por el principio de legalidad penal.

3. Agencia Nacional de Ciberseguridad. Se propone crear una instancia técnica con atribuciones de prevención, coordinación, alerta temprana, gestión de incidentes y enlace con fiscalías, sectores críticos y organismos internacionales. Su diseño debe incluir límites competenciales, controles democráticos, transparencia, protección de datos personales y supervisión judicial cuando sus actuaciones incidan en derechos fundamentales.

4. Régimen de reporte para sectores críticos. Deben establecerse obligaciones de prevención, gestión de riesgos y notificación de incidentes para operadores de sectores críticos. El régimen debe definir sujetos obligados, plazos razonables de reporte, autoridad receptora, medidas de confidencialidad, protección de datos personales y salvaguardas para evitar que la obligación de reportar se convierta en un mecanismo de vigilancia indiscriminada.

Estas cuatro líneas no agotan la agenda legislativa, pero ofrecen un piso mínimo para transformar el diagnóstico en propuestas verificables. Su finalidad es cerrar brechas específicas sin convertir el ciberterrorismo en una categoría expansiva o indeterminada.

Consideraciones finales

El análisis desarrollado permite sostener que México enfrenta un punto de inflexión en materia de seguridad y Estado de Derecho. La convergencia entre violencia estructural derivada del crimen organizado y capacidades disruptivas asociadas al uso de tecnologías digitales configura un escenario de amenazas híbridas frente al cual el marco jurídico vigente resulta insuficiente, fragmentario y conceptualmente ambiguo.

La dimensión digital amplifica el alcance de las conductas intimidatorias, acelera su difusión y facilita que los efectos sociales trasciendan el espacio territorial inmediato. El diagnóstico muestra tipos penales insuficientes, ausencia de definición jurídica de ciberterrorismo, falta de obligaciones exigibles para infraestructura crítica y dificultades procesales para la cooperación internacional en evidencia digital.

La expansión tecnológica del crimen organizado exige una respuesta multidimensional. No basta con actualizar el catálogo de delitos; es necesario construir una arquitectura institucional que permita aplicar las normas de forma efectiva, con cuerpos policiales, fiscales y periciales especializados en cibercriminalidad, evidencia digital e investigación de estructuras criminales complejas.

La dimensión internacional constituye un componente necesario de esta respuesta. La naturaleza deslocalizada del ciberespacio y de las operaciones financieras del narcotráfico desborda los límites territoriales de los códigos penales nacionales, por lo que la cooperación jurídica internacional, el intercambio de inteligencia y la armonización procedimental resultan indispensables.

Por lo tanto, la incorporación de marcos referentes debe ir acompañada de una política de Estado proactiva en la cooperación jurídica internacional, el intercambio de inteligencia y la armonización de procedimientos con otras naciones; de lo contrario, cualquier esfuerzo normativo interno se diluirá ante la primera investigación que requiera cruzar una jurisdicción extranjera.

La efectividad de cualquier respuesta integral depende también de la legitimidad institucional y de la confianza ciudadana. Por ello, cerrar los vacíos normativos debe entenderse como parte de una política de fortalecimiento del Estado de Derecho, sujeta a controles democráticos y compatible con derechos humanos.

La construcción de la resiliencia estatal ante las amenazas híbridas requerirá no solo leyes más precisas y mejor coordinación, sino una política de Estado integral con recursos, formación especializada y controles democráticos efectivos. Los datos empíricos confirman la urgencia: el Índice Global de Ciberseguridad de la UIT (2024) ubica a México en el puesto 52 de 194 países, con calificaciones bajas en marco legal (puesto 78) y coordinación institucional (puesto 65), por debajo de Colombia (36), Chile (44) y Brasil (18) en el contexto latinoamericano (Unión Internacional de Telecomunicaciones, 2024). Los vacíos son concretos y verificables: inexistencia de tipo penal de ciberterrorismo; incapacidad del artículo 211 bis 1 del CPF para subsumir

conductas de finalidad intimidatoria; ausencia de régimen de infraestructura crítica con obligaciones exigibles; falta de mecanismos expeditos de cooperación internacional en evidencia digital; y límites del CNPP para investigar comunicaciones de plataformas extranjeras. Cerrar estas brechas no es un ejercicio de política criminal aislado: es, en términos de Habermas (1998), una condición de legitimidad del Estado de Derecho frente a actores que utilizan precisamente esos vacíos como estrategia de impunidad.

El cierre de estos vacíos normativos requiere algo más que la tipificación de nuevas conductas. Se necesita una respuesta integral basada en definiciones jurídicas estrictas, mecanismos de coordinación interinstitucional e internacional, estándares para sectores críticos, reglas de preservación de evidencia digital y salvaguardas explícitas de derechos humanos.

México enfrenta un entorno en el que la violencia asociada al narcotráfico y los riesgos del ciberespacio pueden converger en amenazas híbridas capaces de tensionar las capacidades estatales y ampliar sus efectos sociales e institucionales.

Una actualización del abordaje jurídico del ciberterrorismo vinculado al narcotráfico debe mantener como eje la protección de derechos humanos, la legalidad penal, el debido proceso, la cooperación técnica multinivel y la construcción de capacidades de resiliencia institucional.

Hablar de ciberterrorismo bajo la figura del narcotráfico no implica trasladar sin matices categorías de seguridad nacional al espacio digital, sino construir un marco jurídico preciso para responder a amenazas híbridas sin sacrificar garantías constitucionales ni ampliar indebidamente el poder punitivo del Estado.

Referencias bibliográficas

Astorga, L. A. (1995). *Mitología del "narcotraficante" en México*. Plaza y Valdés.

Atienza, M. (2013). *El derecho como argumentación*. Ariel.

Bobbio, N. (1960). *Teoria dell'ordinamento giuridico*. Giappichelli.

Buitrago Rincón, P. A., Sánchez Lozano, I., & Mojica Amaya, J. A. (2017). Del terrorismo al ciberterrorismo. En *Escenarios y Desafíos de la Seguridad Multidimensional en Colombia*. Escuela Superior de Guerra. https://doi.org/10.25062/9789585652835

Burbano Bolaños, F. X., & Méndez Herrera, P. N. (2025). Protección jurídica del derecho a la imagen y la voz ante la inteligencia artificial. *Revista Pares - Ciencias Sociales, 5*(2), 126-134. ARK CAICYT: https://id.caicyt.gov.ar/ark:/s27188582/4abmbgmrc

Código Nacional de Procedimientos Penales. (2014, 29 de enero; última reforma 2024). Diario Oficial de la Federación.

Código Penal Federal. (2026). https://www.diputados.gob.mx/LeyesBiblio/pdf_mov/Codigo_Penal_Federal.pdf

Comisión Interamericana de Derechos Humanos, Relatoría Especial para la Libertad de Expresión. (2022). Estándares interamericanos sobre libertad de expresión en entornos digitales. OEA.

Consejo de Europa. (2001). *Convenio sobre la ciberdelincuencia* (ETS No. 185). https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=185

Cossío Díaz, J. R. (2011). La Ley de Seguridad Nacional y el sistema jurídico mexicano. Cuestiones Constitucionales, 24, 23-48.

Dell, M. (2015). Trafficking networks and the Mexican drug war. *American Economic Review, 105*(6), 1738-1779. https://doi.org/10.1257/aer.20121637

Denning, D. E. (2000). Cyberterrorism. Testimony before the Special Oversight Panel on Terrorism, U.S. House of Representatives. https://irp.fas.org/congress/2000_hr/00-05-23denning.htm

Ferrajoli, L. (2011). Principia iuris: Teoría del derecho y de la democracia (Vol. 1). Trotta.

Gobierno de México. (2017). *Estrategia Nacional de Ciberseguridad*. https://www.gob.mx/cms/uploads/attachment/file/271884/Estrategia_Nacional_Ciberseguridad.pdf

Habermas, J. (1998). *Facticidad y validez*. Trotta.

Hernández Sampieri, R., Fernández Collado, C., y Baptista Lucio, P. (2014). *Metodología de la investigación* (6.a ed.). McGraw-Hill.

Lessing, B. (2018). *Making peace in drug wars: Crackdowns and cartels in Latin America*. Cambridge University Press. https://doi.org/10.1017/9781108185837

Ley 1273 (2009, 5 de enero). *Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado denominado de la protección de la información y de los datos*. Diario Oficial de Colombia.

Ley de Seguridad Nacional. (2005, última reforma 2020, 26 de diciembre). Diario Oficial de la Federación.

Ley Federal contra la Delincuencia Organizada. (1996, última reforma 2023). Diario Oficial de la Federación.

Ley Federal de Telecomunicaciones y Radiodifusión. (2014, última reforma 2025, 9 de enero). Diario Oficial de la Federación.

Mayer Lux, L. (2018). Una definición de ciberterrorismo. *Revista Chilena de Derecho y Tecnología*, *7*(2), 5-40. https://doi.org/10.5354/0719-2584.2018.51028

Miró Llinares, F. (2012). *El cibercrimen: Fenomenología y criminología de la delincuencia en el ciberespacio*. Marcial Pons.

Naciones Unidas. (2004). *Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional. UNODC.* https://www.unodc.org/documents/treaties/UNTOC/Publications/TOC%20Convention/TOCebook-s.pdf

OCDE. (2019). *Digital evidence across borders: Challenges and solutions*. OECD Publishing. https://doi.org/10.1787/9789264315037-en

Primer Tribunal Colegiado en Materia Penal del Primer Circuito. (2012). Tesis I.1o.P.83 P (10a.). Acceso ilícito a sistemas informáticos. Alcance del tipo penal del artículo 211 bis 1 del Código Penal Federal. *Semanario Judicial de la Federación y su Gaceta*, Libro XIII, t. 3, p. 1920.

Rid, T. (2013). *Cyber war will not take place*. Oxford University Press.

Suprema Corte de Justicia de la Nación. (2016). Tesis 1a./J.

24/2016 (10a.). Terrorismo. Elementos del tipo penal. *Gaceta del Semanario Judicial de la Federación*, Libro 29, t. II, p. 802.

Tirant. (2024). Cibercrimen: ¿qué es y cómo detectarlo? Noticias Tirant. https://tirant.com/noticias-tirant/noticia-cibercrimen-que-es-y-como-detectarlo/

Tribunal Europeo de Derechos Humanos. (2021). Big Brother Watch y otros c. Reino Unido, demanda n.o 58170/13. TEDH.

Trejo, G., y Ley, S. (2020). Votes, drugs, and violence: The political logic of criminal wars in Mexico. Cambridge University Press. https://doi.org/10.1017/9781108596480

Unión Europea. (2022). *Directiva (UE) 2022/2555 del Parlamento Europeo y del Consejo, de 14 de diciembre de 2022 (Directiva NIS2). Diario Oficial de la Unión Europea*, L 333, 1–80.

Unión Internacional de Telecomunicaciones. (2024). *Global Cybersecurity Index 2024. UIT.* https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx